UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Cellular Telephones, Seized From 3441 Cudahy Avenue, Cudahy, Wisconsin 53110 On 06/13/2018, which are described as follows: (1) SAMSUNG SM-G935F, IMEI 353773/08/437015; (2) SAMSUNG S8 SM-G9550, SERIAL NO. R28J72KRJ3D; (3) LG LS675, SERIAL NO. 601CYCVO353259; (4) PALM CELL PHONE, SERIAL NO. P5PE05KA40HW; (5) APPLE IPHONE MODEL A1303; (6) MOTOROLA BOOST MOBILE, SERIAL NO. 364VLN5VR3; (7) SAMSUNG SCH-R351, SERIAL NO. 268435459004658534; (8) LG L5665, SERIAL NO. 510CYXM1324978 (9) APPLE IPHONE A1349; (10) SAMSUNG SPH-L900, MEID 256691486902331958; (11) HTC APA9292, SERIAL NO. HTO5YHL14245; (12) LG VN251, SERIAL NO. 206KPDT1827954; (13) LG RUMOR 2, SERIAL NO. 904CYSF02340214 Cellular Telephones Were Seized By The FBI And Currently In FBI Milwaukee Division Custody

Case No. 18-M-121

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A-1

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment A-2

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 2339B

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Scott Mahloch
Printed Name and Title

Sworn to before me and signed in my presence:

Date: Aug. 8, 2018

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge
Printed Name and Title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF:
CELLULAR TELEPHONES, SEIZED FROM 3441 CUDAHY AVENUE, CUDAHY, WISCONSIN 53110 ON 06/13/2018, WHICH ARE DESCRIBED AS FOLLOWS:
(1) SAMSUNG SM-G935F, IMEI 353773/08/437015;
(2) SAMSUNG S8 SM-G9550, SERIAL NUMBER: R28J72KRJ3D
(3) LG LS675, SERIAL NUMBER 601CYCVO353259;
(4) PALM CELL PHONE, SERIAL NUMBER P5PE05KA40HW
(5) APPLE IPHONE MODEL A1303;
(6) MOTOROLA BOOST MOBILE, SERIAL NUMBER 364VLN5VR3;
(7) SAMSUNG SCH-R351, SERIAL NUMBER 268435459004658534;
(8) LG L5665, SERIAL NUMBER 510CYXM1324978
(9) APPLE IPHONE A1349
(10) SAMSUNG SPH-L900, MEID 256691486902331958
(11) HTC APA9292, SERIAL NUMBER HTO5YHL14245
(12) LG VN251, SERIAL NUMBER 206KPDT1827954
(13) LG RUMOR 2, SERIAL NUMBER 904CYSF02340214
CELLULAR TELEPHONES WERE SEIZED BY THE FBI AND CURRENTLY IN FBI MILWAUKEE DIVISION CUSTODY

Case No. 18-M-121

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR

A RULE 41 SEARCH WARRANT

I, Scott Mahloch being duly sworn, hereby depose and state the following:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search 13 cellular telephones seized pursuant to a Federal Search and Seizure Warrant executed on June 13, 2018, from the residence of WAHEBA ISSA DAIS, at 3441 Cudahy Avenue, Cudahy, Wisconsin 53110. The seized cellular telephones are described as follows:

(1) SAMSUNG SM-G935F, IMEI 353773/08/437015

(2) SAMSUNG S8 SM-G9550, SERIAL NUMBER: R28J72KRJ3D

(3) LG LS675, SERIAL NUMBER 601CYCVO353259

(4) PALM CELL PHONE, SERIAL NUMBER P5PE05KA40HW

(5) APPLE IPHONE MODEL A1303

(6) MOTOROLA BOOST MOBILE, SERIAL NUMBER 364VLN5VR3

(7) SAMSUNG SCH-R351, SERIAL NUMBER 268435459004658534

(8) LG L5665, SERIAL NUMBER 510CYXM1324978

(9) APPLE IPHONE A1349

(10) SAMSUNG SPH-L900, MEID 256691486902331958

(11) HTC APA9292, SERIAL NUMBER HTO5YHL14245

(12) LG VN251, SERIAL NUMBER 206KPDT1827954

(13) LG RUMOR 2, SERIAL NUMBER 904CYSF02340214

(collectively referred to as the DEVICES). The above listed cellular telephones were seized by the FBI on June 13, 2018, and are in the possession of FBI Milwaukee Division and located at 3600 South Lake Drive, St. Francis, WI 53235.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since April 2009. I am currently assigned to the Joint Terrorism Task Force at the Milwaukee Field Office, where I conduct a variety of investigations in the area of counterterrorism in the performance of my duties. I have investigated and assisted in the investigation of matters involving violations of federal law related to domestic terrorism, international terrorism, weapons of mass destruction, the distribution of bomb-making materials, and material support, including in the preparation and service of criminal complaints and search and arrest warrants. I have conferred with colleagues who have received specialized training from the FBI in investigating crimes related to explosives, biological weapons, and weapons of mass destruction.

3. The statements contained in this affidavit are based in part on my personal knowledge, as well as on information provided to me by other law enforcement officers and civilians. This affidavit is being submitted for the limited purpose of securing the requested search warrant, and I have not included each and every fact known to me concerning this investigation.

4. Based on facts set forth in this affidavit, I submit there is probable cause to believe that WAHEBA ISSA DAIS has attempted to provide material support to a foreign terrorist organization in violation of Title 18, United States Code, Section 2339B(a)(1). DAIS is also known by an alias referred to here as "HE." On June 13, 2018, DAIS was charged by criminal complaint with attempting to provide material support or resources to ISIS, in violation of 18 U.S.C. § 2339B(a)(1). On June 26, 2018, DAIS was indicted on two counts of this same crime. I

submit there is also probable cause to search the subject DEVICES for evidence, fruits, and instrumentalities of this crime.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2339B, relating to attempting to provide material support and resources to an FTO. Elements of the offense are the following: The defendant knowingly attempted to provide material support or resources to a designated FTO; the defendant knew that the organization was a designated foreign terrorist organization, that the organization had engaged in or was engaging in terrorist activity or terrorism; and one of the five jurisdictional requirements is satisfied.

THE ISLAMIC STATE OF IRAQ AND AL-SHAM

6. On or about October 15, 2004, the United States Secretary of State designated Al-Qaeda in Iraq (AQI), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization (FTO) Under Section 219 of the Immigration and Nationality Act and Specifically Designated Global Terrorist under section 1(b) of Executive Order 13224.

7. On or about May 15, 2015, the Secretary of State amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and Specifically Designated Global Terrorist under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant (ISIL) as its primary name. The Secretary also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (ISIS—which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria (ISIS), ad-Dawla al'Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On

September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

BACKGROUND OF INVESTIGATION AND FACTS ESTABLISHING PROBABLE CAUSE

8. The FBI Joint Terrorism Task Force has been investigating WAHEBA ISSA DAIS (DAIS) as a suspect involved in the provision of material support to ISIS, in violation of 18 U.S.C. § 2339B. As of March 2017, the FBI became aware that DAIS was promoting ISIS via multiple social media platforms such as Twitter, Facebook and Telegram. The investigation has revealed that DAIS, through the use of multiple social media accounts that she has hacked and taken over from unwitting victims and private social media platforms, promotes ISIS ideology, recruits adherents to ISIS, advocates that her followers conduct attacks in the name of ISIS, collects information on how to make explosives and biological weapons and on how to conduct terrorist attacks, and distributes that information to individuals so they can conduct attacks on behalf of ISIS. For instance, DAIS used one of her pro-ISIS Facebook accounts (an account she hacked and took over from an unwitting victim) to direct an individual, whom she believed to be an ISIS supporter planning to conduct an attack in the name of ISIS, to her password-protected social media channel to find instructions on how to make Ricin and then suggested the individual introduce the Ricin to a government post or water reservoirs.

9. According to information provided by the Department of Homeland Security, DAIS was born on or about August 22, 1972, in Jerusalem, Israel, and was allowed to enter the United States without a passport arriving in Chicago, Illinois (via Paris, France), in approximately November 1992 because of her marriage to a U.S. Citizen (her husband filed for divorce in 2003). On DAIS's visa application, she indicated she intended to stay in the United States permanently as a housewife; that she was from Jerusalem; and that she could speak, read, and

write in English and Arabic. DAIS is now a Lawful Permanent Resident of the United States and lives in Cudahy, Wisconsin, with five of her children, including three minors.

10. The FBI's investigation indicates that DAIS uses multiple Facebook, Twitter, identified social media, and email accounts that contain pro-ISIS statements and information on how to make biological weapons, explosives, and explosive vests. As explained in more detail below, in approximately January 2018, Facebook Security informed the FBI that a Facebook user with an identified screen name (referred here to as HE) and User Identification number (UID) ending in 1813 appeared to be a Wisconsin-based user posting detailed instructions on how to make explosive vest bombs in support of ISIS. This Facebook user also appeared to be engaged in detailed question and answer sessions discussing substances used to make bombs. As also discussed more fully below, FBI investigation has determined this user was DAIS. Further investigation has revealed that DAIS has used multiple social media platforms to pledge allegiance to ISIS, promote ISIS's terrorist agenda, communicate with ISIS members overseas, facilitate and encourage recruitment and attack planning for ISIS, and distribute instructions on explosives and biological weapons to self-proclaimed ISIS members and to people she believed to be planning to conduct attacks on behalf of ISIS. The investigation has revealed that DAIS hacks Facebook accounts, taking them over from unwitting victims and changing the profile picture, friends list, and display name. FBI investigation has identified the following Facebook accounts as being used by DAIS to attempt to provide material support to ISIS, distribute information on bomb-making and recipes for Ricin, and facilitate attacks: UID ending in 1813, UID ending in 4063, UID ending in 2942, and UID ending in 6059. These four accounts are not an exhaustive list of all the accounts DAIS has hacked and taken over as her own.

11. Based on the FBI investigation, I believe that DAIS, who has pledged her allegiance to ISIS, is actively promoting ISIS propaganda through social media channels in an attempt to radicalize and recruit ISIS members and to encourage ISIS supporters to conduct terrorist attacks. I further believe that DAIS has helped facilitate planning for attacks in the United States on behalf of ISIS and overseas by providing instructions on how to make explosives, biological weapons, and suicide vests, and providing detailed instruction to people interested in attacks and attack planning. DAIS has also expressed a personal desire to travel overseas in support of ISIS.

DAIS'S HACKING OF VICTIM FACEBOOK ACCOUNTS

12. Open source searches and information provided by Facebook pursuant to 18 U.S.C. § 2702 indicate that DAIS and the individuals who are communicating with DAIS on Facebook are using hacked Facebook accounts as a way to avoid law enforcement detection of their communications. When DAIS takes over a Facebook account, she changes the display name to a variant of HE (written in English and/or Arabic) and changes the profile picture. The profile picture used by DAIS on these hacked Facebook accounts was taken by a professional photographer and is of a young girl wearing a blue dress. The photograph was taken as part of a series documenting Yazidi, a minority population in northern Iraq, fleeing their hometown to escape violence caused by the Islamic State militants. This photograph can be found on the internet.

13. On or about January 11, 2018, an FBI confidential source (Source #1)[1] reported that DAIS is unemployed and has her Islamic husband (which means married by their religion and

[1] Source #1 was opened in approximately January 2018. Some of his/her reporting has been corroborated, he/she has direct access through a sub-source, and he/she is considered reliable. To date, Source #1 has not been paid and is motivated by not wanting to lose his/her ability to obtain a Top Secret clearance for employment due to his/her association with the subject. Source #1 was applying for a position that required a TS clearance.

not law) pay the bills. Source #1 described DAIS as constantly on social media promoting ISIS and using an identified social media application to talk to "shady people" in the Middle East on a regular basis. Source #1 reported that DAIS uses accounts on Twitter and Facebook, but they are always being shut down due to her posting pro-ISIS propaganda. According to Source #1, DAIS also has numerous "throw away" e-mail addresses to create all these accounts. Source #1 stated that DAIS has a YouTube account that she subscribes to and possibly creates videos on how to hack into social media accounts and is able to crack passwords for Facebook accounts. As discussed below, FBI investigation has confirmed that DAIS hacks into Facebook accounts belonging to others, as an operational security measure, and uses those accounts to promote ISIS and to facilitate ISIS recruitment and attack planning.

14. The FBI's investigation has identified multiple Facebook accounts hacked by DAIS. The following list of accounts includes examples of the multiple accounts and is not exhaustive. The information below was provided to the FBI pursuant to legal process, publicly available information, and open source research.

15. Review of account information received pursuant to legal process shows that Facebook account with UID ending in 1813 and display name (HE) was used to pass information on how to build explosives to members of ISIS. FBI investigation has revealed that the account previously belonged to an unrelated female (Victim No. 1) but was hacked and taken over by DAIS in approximately January 2018. According to Facebook, UID ending in 1813 was created in approximately January 2012 by a female in Carabobo, Venezuela. On or about January 4, 2018, the account's display name was changed to HE and the majority of the original friends were removed from the account. The same day, the account quickly began to add a large number of new friends. The account profile picture used was the distinct photo of the young girl in a blue

dress that was previously discussed. After the account name was changed, it was frequently accessed from an Internet Protocol (IP) address that resolved to DAIS's residence at 3441 Cudahy Avenue, Cudahy, Wisconsin 53110. It is noted that on or about January 8, 2018, while using UID ending in 1813 to exchange private messages, DAIS provided email address baqyyia22@xxx.com as a means to contact her outside of Facebook. At that time, this email address was associated with DAIS and a phone number that was subscribed to by DAIS. Based on prior investigation and source reporting, I believe DAIS is the user of UID ending in 1813.

16. On or about January 23, 2018, investigators conducted an open source search of DAIS's alias, HE, and identified UID ending in 4063, which also appears to have been hacked and taken over from a female in Venezuela (Victim No. 2). My review of publicly available information on this account revealed it had the same distinct profile picture as UID 1813. The account was previously used by a female whose profile showed she studied at a University in Carabobo, Venezuela. Review of account information received pursuant to legal process shows this account was created in approximately January 2012, and on or about January 8, 2018, the friends from the original account were removed. On or about January 23, 2018, the account name was changed to a variant of HE and new friends began to be added. After the name of the account was changed, it was accessed frequently from an IP address that resolved to DAIS's residence at 3441 Cudahy Avenue, Cudahy, Wisconsin 53110. Based on prior investigation and source reporting, I believe DAIS is the user of UID ending in 4063.

17. On or about March 2, 2018, an FBI Undercover Employee (UCE) looked up Facebook user name HE and discovered Facebook account with UID ending in 2942 with that name and DAIS's distinct profile picture. The UCE's review of UID ending in 2942 showed the subscriber is from Venezuela (Victim No. 3). The UCE sent DAIS a private message, asking for advice and

DAIS provided email address baqyyia22@gmail.com to the UCE as her email address. Google's response to legal process also indicated that the email address baqyyia22@gmail.com was primarily accessed from an IP address that resolves to DAIS's residence. Based on the foregoing, I believe DAIS uses Facebook account UID ending in 2942.

18. On or about April 23, 2018, investigators conducted an open source search of HE in Arabic and identified Facebook account UID ending in 6059 under the display name of a variant of HE The account had the same distinct profile picture that DAIS is known to use. The profile indicates the subscriber is from Camp Grande, Brazil, and includes pictures of a young male. The rest of the account is in Arabic. IP address records obtained via Grand Jury subpoena indicate that the IP address used to access the account resolved to DAIS's residence at 3441 Cudahy Avenue, Cudahy, Wisconsin 53110. I believe that this account was previously used by Victim No. 4 and then hacked by DAIS on or about April 12, 2018, when the cover photograph was changed to DAIS' distinct photograph.

DAIS'S PLEDGES OF SUPPORT TO ISIS

19. DAIS has pledged her allegiance to ISIS on numerous occasions. On or about February 12, 2018, DAIS (using Facebook UID ending in 4063) posted on her Facebook wall, confirming that her posts are her beliefs and that she believes in the doctrine of ISIS: "#Caution. When I publish any statement I completely believe in it. I was and I continue to be on the doctrine of the Islamic State." DAIS (using Facebook UID ending in 4063) posted on her Facebook wall on or about February 10, 2018, a post titled "#Renewal of the pledge of allegiance one more time." DAIS wrote, "I pledge allegiance to Ameer al Mumineen [the commander of the faithful] Ibrahim al-Husaini al-Qarashi, [Abu Bakir al-Baghdadi] to listen and obey in what is desirable and undesirables and in times of hardship and prosperity, and to endure being discriminated

against and to not dispute the orders of those in charge, unless I witness a clear apostasy, for which Allah has shown me a clear proof, and Allah is my witness." In response to this post, seventeen of her friends commented pledging their allegiance to ISIS as well.

20. A review of information provided from Facebook pursuant to 18 U.S.C. § 2702, identified a conversation on or about January 7, 2018, between DAIS (using Facebook UID ending in 1813) and another self-proclaimed ISIS supporter (referred to here as AK) in which they discussed allegiance to ISIS and traveling to join ISIS. DAIS claimed she was born in the United States and was living there. She told AK that she had pledged allegiance to ISIS and was seeking a way to join ISIS in Syria but is forbidden from leaving the country. She further informed AK that an ISIS military trainer in Raqqa, Syria, was trying to assist her in getting to Syria via Turkey. DAIS declared she follows the path and ideology of the Islamic State and that she would not bow for any tyrants. She stated this numerous times throughout the conversation with AK. AK declared that he is a supporter of ISIS as well.

21. In this same conversation, DAIS told AK that she wanted to leave America, but could not and if she tried to leave, she would be arrested for "conspiracy to join." DAIS said that she prayed that Allah would facilitate her exit and that she may "try in a few months." AK told her that they "may end up in Paradise." DAIS told AK that she knew some brothers from Diwan (believed to refer to the ISIS Ministry) and that she had inquired and learned that she can travel to join ISIS without a male escort, which she did not have. DAIS stated she had an ISIS contact in Al-Raqqah who had told her to travel to Turkey and that he would arrange for a male escort to meet her, but then the individual left for Al-Barakah and was "martyred." She said that she had seen videos of him training soldiers online.

22. DAIS has pledged her allegiance to ISIS and has been praised by others for her online support of ISIS via Facebook account UID ending in 1813. For instance, on or about January 5, 2018, a Facebook user (referred to as AA) sent DAIS a private message that stated, "All your postings are in the service for Jihad and the Mujahidin. God bless you." On or about January 14, 2018, DAIS exchanged private messages with the user of Facebook UID ending in 4904 (referred to as AS) about restoring Facebook accounts that had been suspended. DAIS said, "May God keep you safe" to which AS responded, "and may you stay with us on Facebook forever." DAIS said, "except…May God grant me martyrdom and I leave the Facebook." AS responded by telling DAIS that "we are in jihad to spread this message and the truth. As long as the message is God you will be rewarded... all of us wish for and ask God to grant us martyrdom." On or about January 24, 2018, DAIS (using Facebook UID ending in 4063) posted on her Facebook wall urging people to add #The_Supporters_Campaign to their friends list. The user of another Facebook account (Facebook User No. 7) responded by declaring DAIS a supporter of ISIS and very knowledgeable.

DAIS'S PROMOTION AND RECRUITMENT ACTIVITIES ON BEHALF OF ISIS

23. DAIS has used social media on multiple occasions to promote ISIS and its terrorist agenda and to attempt to recruit others to join ISIS and to commit attacks on behalf of ISIS. On or about January 30, 2018, the UCE conducted an open source search of DAIS's alias, HE, and identified Facebook account UID ending in 4063. Subsequently the UCE sent a friend request to that account and it was accepted that day. The UCE then was able to view the Facebook wall of UID ending in 4063. The UCE noted that DAIS had posted the following in Arabic: "#Attention

to the non-#supporters brothers: I accepted your friend requests hoping that Allah will guide at least one of you [to become a supporter]."

24. On or about February 24, 2018, DAIS (using Facebook UID ending in 2942) posted a link to a social media channel entitled, "Khilafah Ray for Supporters Group." I believe Khilafah refers to the Caliphate, also known as ISIS. The UCE visited the channel on February 26, 2018, and noted that the page had multiple voice messages posted by DAIS's social media account @ISWarrior and they consisted of Jihadi songs and speeches by ISIS leaders. One of the messages encouraged ISIS supporters who cannot travel to ISIS-controlled areas to conduct terrorist attacks in the countries where they reside. If military targets are not in their reach, then attacks directed at civilians are even more desirable by ISIS.

25. On or about January 23, 2018, DAIS (using Facebook UID ending in 4063) posted on Facebook that her social media channel, "The Caliphate's Ray," had been removed. She then posted links to two social media channels. A Facebook user (referred to here as II) posted that it suits DAIS well to be the press manager for ISIS. II continued to praise DAIS for her perseverance, efforts, and exemplary support of ISIS.

26. A review of information provided from Facebook on or about February 6, 2018, pursuant to 18 U.S.C. § 2702, identified a Facebook user (referred to here as OG) who was planning a potential ISIS attack and had been communicating with DAIS (using Facebook account with UID ending in 4063) about the attack. On or about January 26, 2018, OG asked DAIS if she knew about Sharia. DAIS responded by stating that OG should ask the question and DAIS would send it to an expert for an answer. OG stated that he would be traveling to France. He then said it would be better to die than rot in prison. He asked how he can take revenge for ISIS. He suggested running a car through people or shooting at people. He then asked how he would be

judged by God after killing many people. DAIS responded that she will send him an answer later. On or about January 27, 2018, DAIS sent a link to a Facebook profile (referred to here as SM) and told OG to talk to this individual, that he will be beneficial to OG.

27. On or about January 28, 2018, OG and SM exchanged private Facebook messages. OG said he was a 25-year-old Algerian who had previously discussed plans with HE (using a short form for DAIS's alias) to travel to France. He said he wanted to plan an operation in support of ISIS so DAIS suggested he talk to SM. SM then sent OG the following pledge to ISIS: "Renewal of the pledge of allegiance, we are renewing the pledge of allegiance to Sheikh Abu Bakr Al-Bughdadi [sic] to obey him in everything, not to go against his will, not to flee during the fight, not to deny the religion of God and God is our witness." OG requested weapons and brothers to help with his attack. SM reminded OG that the work is individual. On or about January 30, 2018, OG sent DAIS a message saying that DAIS is really knowledgeable.

DAIS'S DISTRIBUTION OF EXPLOSIVES & BIOLOGICAL WEAPONS INFORMATION

28. DAIS has distributed information pertaining to explosives and biological weapons on Facebook and other social media platforms in the form of videos and conversations about bomb-making and biological weapons materials. In particular, DAIS has used Facebook UID ending in 1813 to distribute information on how to build explosives and biological weapons so that people who want to commit violent acts in the name of ISIS will use this information to commit acts of violence. DAIS promotes violent acts in the name of ISIS on her Facebook pages to her Facebook friends who are self-proclaimed ISIS members and supporters. For instance, one friend of account ending in UID 1813 (Facebook User No. 8) has instructions for creating explosives and Ricin on his page and photographs that include the ISIS flag. On or about January 16, 2018, another friend of this account (Facebook User No. 9) engaged in a private message conversation

with DAIS (using Facebook UID ending in 1813) in which he said he had been with ISIS for years and told her about specific battles and described the battlefield in detail. As described above, in a private message conversation with DAIS (using Facebook UID 1813), AK declared that he is a supporter of ISIS as well.

29. DAIS has posted numerous videos about explosives on Facebook. On or about January 8, 2018, DAIS posted a video on her Facebook page with UID ending in 1813. The video is a presentation from "Sawt al-Jihad" (translated as "The Voice of Jihad") and titled, "Explosive Belt/Vest." The video purports to provide step-by-step instructions on how to make an explosive belt and then demonstrates the effect of the bomb when it explodes. Audio in the background plays a chant in support of Jihad. On or about January 11, 2018, DAIS posted a video on the Facebook page for UID ending in 1813. The video is titled, "The Practical Training in the Making of Ammonium Nitrate." The video purports to provide step-by-step instructions on how to make Ammonium Nitrate. On or about January 11, 2018, DAIS posted a video on the Facebook page for UID ending in 1813. The video is titled, "The Practical Training in the Making of TNT."[2] The video purports to provide step-by-step instructions on how to make TNT. Audio in the background plays a chant in support of jihad.

30. DAIS continually seeks to collect information on the best explosives and biological weapons techniques in order to pass this information on to would-be ISIS attackers. On or about January 8, 2018, DAIS used Facebook UID ending in 1813 to communicate with a Facebook user (referred to here as AO) about explosive vests. AO told DAIS that ISIS made a safer and more reliable explosive belt. AO explained that they do not use electronic detonators because they are dangerous and may explode prematurely and suggested a grenade with a fuse. DAIS

[2] I know that TNT is Trinitrotoluene, a chemical compound that is a high explosive.

asked if he had any videos or written instructions that he could share with her. AO then began to discuss plans to kill Jews overseas. At that point, DAIS suggested that AO not discuss such topics on Facebook because they are probably being monitored.

31. On or about January 9, 2018, DAIS (using Facebook UID ending in 1813) had a detailed conversation with AK about substances used to create bombs. On or about January 9, 2018, DAIS posted on her Facebook wall that Nitric Acid[3] can be found in gold stores but that a clearance is required to purchase it. DAIS recommended producing it because it is difficult to purchase. She then asked where it can be purchased in the Arab Peninsula. She proceeded to ask for the names of commercial fertilizers that would not trigger suspicion when asked about. She posted within the comments that she had heard that nitric acid is used to melt gold so she wanted to know if it could be purchased from gold stores and if that would raise suspicion. DAIS then asked that someone try to purchase nitric acid from a pharmacy after someone suggested it could be purchased that way. DAIS also recommended researching where to get instant fertilizer in Western countries. She then asked if there are nitrates in Potassium Nitrate. AK responded that Ammonium Nitrate[4] needs to be extracted from fertilizer because it is sold in large quantities to land owners. He recommended that this would make a good security cover. If asked questions, AK suggested that DAIS say she does not understand chemicals but is merely a farmer.

32. DAIS has attempted to provide material support to ISIS by providing detailed instructions on how to make Ricin to an individual seeking to commit an attack in the name of ISIS.

---

[3] I know that Nitric Acid is a strong acid chemical compound that carries oxygen atoms. It can be used to oxidize or provide oxygen to other chemicals utilized in explosives.

[4] I know that Ammonium Nitrate is a chemical compound that is a strong oxidizer often used in explosives.

33. In particular, on or about March 2, 2018, the UCE sent a private message to DAIS (using Facebook UID ending in 2942) requesting her permission to discuss a sensitive and important topic that the UCE needed her opinion on. DAIS thanked the UCE for his/her confidence and trust. She encouraged the UCE to share his question. The UCE told DAIS that he/she had anticipated completing his/her master degree in a year, but could no longer stand living in the land of the infidel. The UCE stated he/she constantly clashed with colleagues and felt that government spies were everywhere. DAIS responded saying, "I am reading your words and unfortunately, you are causing your own demise by clashing with them. We live in a time where you do not know when you are going to be stabbed in the back. And I don't think the Islamic State would want its supporters be thrown in infidels' prisons. We cannot be of benefit to them like that." DAIS asked if the UCE knew why the September 11th attacks were successful and then answered it was due to their total secrecy. DAIS instructed the UCE to plan and not leak information. DAIS further stated, "[T]hey do not need any evidence. Just a tip and a suspicion. If someone says that this belongs to a terrorist group, they will come to your house, handcuff you and take you."

34. DAIS instructed the UCE to stay away from others, not discuss this idea with others, and secure the UCE's social media account. DAIS also told the UCE that he/she must act like an ordinary person. She also advised the UCE to not act interested in these topics and if someone asked about it, the UCE should tell them these topics do not interest him/her. DAIS emphasized that total secrecy is the most important thing and that the UCE must take time in planning, choosing a target, and studying it well from all aspects, even if it takes months.

35. DAIS told the UCE it is hard to join the [Islamic] State because they do not have much land under their control and instead it is better to execute an attack where you are. DAIS

suggested potential targets for attacks, such as street festivals and celebrations in the summer, or churches. DAIS also advised that it should be something that would devastate and kill more than one person. Further, she said, "Learn how to make bombs and explosive belts as a preparation process. They've been talking about this for months." After the UCE said he/she has no experience making weapons or explosives, DAIS said, "No problem, making bombs is easy, and you can also start with poisons. I have a [social media] Channel you may benefit from." She further said, "I advise you to use poisons first" and then she again recommended her channel as a place to find an encyclopedia of poisons. DAIS told the UCE to let her know if the UCE needed help. She said the easiest poison to make is Ricin, which she claimed is very effective and lethal to the touch. DAIS then sent a link to the social media channel and said, "Lessons in making explosives and everything related to Lone Wolves, may Allah make us beneficial." DAIS then asked, "Remember Boston Marathon bombing?" The UCE responded affirmatively, and DAIS said, "It was very easy to make. All it needs is a pressure cooker, shrapnel and explosives. Join my channel and research." The UCE asked if there were any poison recipes DAIS could send to the UCE, and DAIS responded, "Yes. I will send you the poison of Ricin for it is easier, more effective, and can not be traced, even if the person dies, it can not be found in the body. All you need is just two items." DAIS then said, "Castor seeds and Acetone." The UCE and DAIS then exchanged email addresses.

36. On or about May 2, 2018, the UCE and DAIS exchanged private messages via Facebook. The UCE asked DAIS about her social media channel titled, "Shu'a' Al-Khilafah for lone wolves." I believe Al-Khilafah refers to the Caliphate, aka ISIS. DAIS responded by providing a new link to a social media channel and stating that the link is not publicly available to members but rather just to the administrators. The UCE's review of the channel revealed that it is directed

to "lone wolves" making poisons, explosives, weapons, and silencers. I believe that "lone wolves" refers to individuals who are inspired by one or more terrorist groups to commit attacks acting on their own. The channel has 89 members, four photos, 10 videos, 445 files and one shared link. The translated titles of the 92 documents the UCE pulled down all relate to explosives, guns, attack planning, and target selection.

37. On or about May 3, 2018, the UCE sent a private message to DAIS via Facebook account UID ending in 2186. The UCE asked if the account was the account of a variant of HE to which DAIS responded in the affirmative. The UCE said that he/she had downloaded the Ricin file from DAIS's social media channel. DAIS said, "Good. May Allah make you successful. It's easy to make but remember to be cautious." DAIS continued to provide the UCE with advice such as wearing multiple gloves and covering the surface of the work table "because it's lethal to the touch." In discussing potential targets, DAIS suggests a government post or placing it in water reservoirs. During the conversation, DAIS told the UCE that she resides in the United States. The UCE asked DAIS if it was easy to travel to the Unites States and suggested there might be more targets in the United States. DAIS agreed and said there are many opportunities in the United States. DAIS offered that they could work together. Ricin is a biological toxin made from the castor bean.

38. A review of information provided from Facebook on or about May 11, 2018, pursuant to 18 U.S.C. § 2702, identified a conversation between DAIS (using Facebook UID ending in 2942) and a Facebook user (referred to here as EAR). EAR told DAIS, "I am in need of a way to build explosives by using agricultural fertilizer." DAIS replied, "Participate in my channel about explosives" and then provided a link to her channel titled "The ray of the Khilafa- Explosives: Lone Wolves." The summary included with the link described the channel as providing

"[l]essons in manufacturing of explosives and everything regarding Lone Wolves." EAR said that he would like to "build a bomb that can uproot a whole house. I am confused on which one to pick, and don't know how to formulate in grams of explosives and how to make it powerful." DAIS advised EAR that he needed to "start with a small amount, meaning don't make the whole thing at once. You have to experiment with small quantities and then make it bigger." EAR thanked DAIS for her advice.

PROBABLE CAUSE TO SEARCH THE SUBJECT DEVICES

ARREST OF DAIS AND EXECUTION OF SEARCH WARRANT

39. As noted above, on June 13, 2018, DAIS was charged by criminal complaint with attempting to provide material support or resources to ISIS, in violation of 18 U.S.C. § 2339B(a)(1). On that same date, a federal search and seizure warrant was executed at DAIS's residence at 3441 Cudahy Avenue, Cudahy, Wisconsin 53110. Each of the subject DEVICES was seized during the execution of that warrant. The subject DEVICES were taken into FBI custody and are being stored in evidence at FBI Milwaukee Division, located at 3600 South Lake Drive, St. Francis, WI 53235.

40. During the execution of the federal search warrant on June 13, 2018, agents observed that the residence is a one story structure, comprised of two floors, a main floor, and a basement. The first floor has a living room, kitchen, dining room, bathroom, and three bedrooms (Bedroom #1, Bedroom #2, and Bedroom #3). The basement has two rooms, a large room that takes up the majority of the basement and a bedroom (Bedroom #4). None of the rooms on the main floor has doors for the rooms, as verified through agents conducting the arrest and search, and through photos taken of the residence during the search. The residence houses a total of six people, three adults—DAIS and her two sons ages 18 (Adult Child #2) and 22 (Adult Child #3)—and three

minor children ages 5, 12, and 13. It is believed that Adult Child #3 lives in Bedroom #4. It is unknown which bedrooms DAIS, the three minor children, and Adult Child #2 have used.

41. The following is a list of the DEVICES and where they were found during the execution of the Federal Search Warrant on June 13, 2018, at DAIS's residence at 3441 Cudahy Avenue, Cudahy, Wisconsin. The DEVICES and their pictures are contained in Attachment A-1.

(1) SAMSUNG SM-G935F IMEI 353773/08/437015 – Bedroom #1

(2) SAMSUNG S8 SM-G9550, SERIAL NUMBER: R28J72KRJ3D – Bedroom #3

(3) LG LS675 SERIAL NUMBER 601CYCVO353259 – Bedroom #1

(4) PALM CELL PHONE SERIAL NUMBER P5PE05KA40HW – Bedroom #2

(5) APPLE IPHONE MODEL A1303 – Bedroom #1

(6) MOTOROLA BOOST MOBILE SERIAL NUMBER 364VLN5VR3 – Bedroom #1

(7) SAMSUNG SCH-R351 SERIAL NUMBER 268435459004658534 – Bedroom #1

(8) LG L5665 SERIAL NUMBER 510CYXM1324978 – Bedroom #2

(9) APPLE IPHONE A1349 – Bedroom #1

(10) SAMSUNG SPH-L900 MEID 256691486902331958 – Bedroom #4

(11) HTC APA9292 SERIAL NUMBER HTO5YHL14245 – Bedroom #4

(12) LG VN251 SERIAL NUMBER 206KPDT1827954 – Bedroom #4

(13) LG RUMOR 2 SERIAL NUMBER 904CYSF02340214 – Bedroom #4

SAMSUNG SM-G935F IMEI 353773/08/437015

42. During the interview of DAIS following her arrest on June 13, 2018, DAIS told interviewing agents she previously had owned a Samsung S7 Edge. DAIS indicated she reformatted this phone and gave it to Child #1 to play with. Adult Child #1 was interviewed by FBI Milwaukee agents on June 13, 2018. Adult Child #1 also told investigators DAIS recently

gave her old phone to one of Adult Child #1's siblings. During a recorded jail call from Waukesha County Jail between DAIS and Child #1 on June 16, 2018, DAIS asked if Child #1 had deleted all DAIS's stuff from the phone when DAIS gave it to Child #1. Child #1 responded to DAIS that Child #1 had deleted everything except the pictures, per DAIS's instructions. Online research using the term Samsung SM-G935F revealed that this device is referred to as a Samsung S7 Edge. The Samsung SM-G935F listed below in Attachment A-1 as item (1) is believed to be the Samsung S7 Edge referred to by DAIS in the June 13, 2018 interview.

REMAINING DEVICES

43. During an interview on June 13, 2018, Adult Child #1 stated there was no privacy within the house due Adult Child #1's autistic brother's aggressive outbreaks, during which he breaks items in the house, including damage to doors, resulting in all doors being removed from the main floor of the residence. Adult Child #1 indicated that DAIS and members of the family residing in the home have no specific areas that are set aside for themselves as "private areas." During a recorded jail call from Waukesha County Jail between DAIS and Adult Child #1 on June 16, 2018, DAIS stated the doors in the house were all broken.

44. During an interview of Child #1 on June 20, 2018, Child #1 told a FBI Child/Adolescent Forensic Interviewer (CAFI) that DAIS purchased different cellular telephones when she had money. Child #1 stated during the interview that DAIS's old phones would be given to her children. In a separate interview of Child #2, which was also conducted by CAFI on June 20, 2018, Child #2 stated that another one of DAIS's children, Adult Child #2, has one of DAIS's old phones.

45. The FBI will perform a preliminary review of each of the above-listed DEVICES to determine if DAIS has used any of the DEVICES. If it is determined DAIS did not use any particular DEVICE, the FBI will discontinue its search of that DEVICE.

46. There is probable cause to believe that the items listed in Attachment A-2 will be found on the DEVICES:

a. As described above, DAIS's activities in support of ISIS mainly have been conducted online. The subject DEVICES are smartphones that are cable of accessing the Internet, which was available via wireless Internet throughout the residence.

b. In conducting her material support activities, DAIS has used social media applications such as Facebook. These social media applications have mobile applications that can be used on cellular telephones.

c. Based on my training and experience, I know that ISIS supporters use their cellular telephones to facilitate attack planning, to communicate with like-minded associates and to access encrypted applications in order to evade law enforcement, as I believe DAIS has done.

d. Similarly, I know those communicating with like-minded associates to further spread extremist ideologies and propaganda or to facilitate attack planning, often use multiple personal electronic devices or cellular telephones to evade law enforcement detection. In this case, DAIS is known to have used multiple cellular telephones and to have given her old phones to her children. She also is believed to have attempted to erase information on at least one of these old phones.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

47. As described above and in Attachment A-2, this application seeks permission to search for records that might be found on the cellular telephones, in whatever form they are found. One

form in which the records might be found is data stored on the DEVICES. Thus, the warrant applied for would authorize the searching of these DEVICES or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

48. *Probable cause*. I submit that if a storage medium is found on the DEVICES, there is probable cause to believe relevant records will be stored on that DEVICE or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium.

b. Deleted files, or remnants of deleted files, thus may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a DEVICE operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, storage media—in particular, a DEVICES' internal hard drives—contain electronic evidence of how a DEVICE has been used, what is has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files.

Cellular telephone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

49. *Forensic evidence*. As further described in Attachment A-2, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cellular telephones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any cellular telephone or because:

a. Data stored on the cellular telephones can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of other storage DEVICE or other external storage media, and the times the cellular telephone was in use. Cellular telephone file systems can record information about the dates files were created and the sequence in which they were created, although this information later can be falsified.

b. Information stored within a cellular telephone may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a

cellular telephone (e.g., registry information; communications; images and movies; transactional information; records of session times and durations; internet history) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the device was remotely accessed, thus inculpating or exculpating the cellular telephone owner. Further, cellular telephone storage media activity can indicate how and when the device or storage media was accessed or used. For example, cellular telephones typically contain information that log: user account session times and durations, activity associated with user accounts, electronic storage media that connected with the cellular telephone, and the IP addresses through which the cellular telephone accessed networks and the internet. Such information allows investigators to understand the chronological context of cellular telephone or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a cellular telephone may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such images files, along with external device connection logs, also may indicate the presence of additional electronic storage media. The geographic and timeline information may either inculpate or exculpate the computer user. Further, information stored within a cellular telephone may provide relevant insight into the cellular telephone user's state of mind as it relates to the offense under investigation. For example, information within a cellular telephone may indicate the owner's motive and intent to commit the crime or consciousness of guilt.

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper contest, draw conclusions about how cellular telephone were used, the purpose of their use, who used them, and when.

d. Further, in finding evidence of how a cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish a particular thing is not present on a storage medium.

50. *Necessity of seizing or copying entire cellular telephone.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. Seizures or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

51. *Search of Subject DEVICES*: Based on my knowledge, training, and experience, I know that cellular telephones can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools for the same reasons as those listed.

CONCLUSION

52. I submit that this affidavit supports probable cause for a search warrant authorizing the search of the seized cellular telephones as described and pictured in Attachment A-1, for the items described in Attachment A-2.

Respectfully submitted,

Scott Mahloch
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August 8th, 2018

HON. DAVID E. JONES
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

1. The property to be searched consists of the following cellular telephones, seized from 3441 Cudahy Avenue, Cudahy, Wisconsin on 06/13/2018 and are currently housed within FBI Milwaukee Division evidence, located at 3600 South Lake Drive, St. Francis, WI 53235.

(1) SAMSUNG SM-G935F, IMEI 353773/08/437015

(2) SAMSUNG S8 SM-G9550, SERIAL NUMBER R28J72KRJ3D

(3) LG LS675, SERIAL NUMBER 601CYCVO353259

(4) PALM CELL PHONE, SERIAL NUMBER P5PE05KA40HW

(5) APPLE IPHONE MODEL A1303

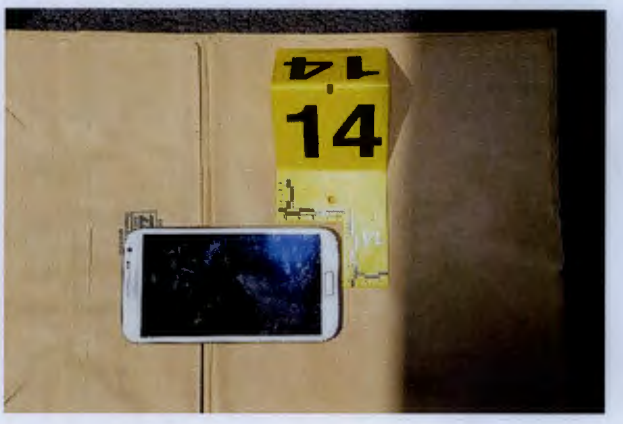
(6) MOTOROLA BOOST MOBILE, SERIAL NUMBER 364VLN5VR3

(7) SAMSUNG SCH-R351, SERIAL NUMBER 268435459004658534

(8) LG L5665, SERIAL NUMBER 510CYXM1324978

(9) APPLE IPHONE A1349


(10) SAMSUNG SPH-L900, MEID 256691486902331958




(11) HTC APA9292, SERIAL NUMBER HTO5YHL14245


(12) LG VN251, SERIAL NUMBER 206KPDT1827954

(13) LG RUMOR 2, SERIAL NUMBER 904CYSF02340214

ATTACHMENT A-2

1. All records on the cellular telephones described in Attachment A-1 that relate to violations of Title 18 United States Code, Section 2339B, and involving WAHEBA ISSA DAIS, and others since March 2017, including any and all records relating to:

a. Any information in any form that is related to terrorism or a threat the national security of the United States;

b. Evidence of loyalties to a foreign power;

c. Pictures of weapons, ammunition, tactical equipment, tactical or camouflage clothing, explosives, explosives devices, explosive precursor chemicals, incendiaries; incendiary devices, incendiary chemicals or precursor chemicals and any other hazardous devices or substances deemed relevant to the investigation;

d. Pictures of flags, banners, patches, specifically designed clothing that depicts the symbol of a terrorist groups or terrorist movements;

e. Recorded forms of identification, journals, and diaries;

f. Travel documents and indicia of travel overseas and domestically, including airline tickets, passports, visas, hotel records, and travel itineraries;

g. Calendars, time schedules, address books, and contact list information;

h. Financial information to include all financial institution records, checks, credit or debit cards, automated teller machine cards, public benefit program cards, account information, other financial records, financial instruments and moneys;

i. Evidence of money orders, wire transfers, cashier's check receipts, bank statements, passbooks, checkbooks, and check registers pertaining to travel overseas, the Islamic State of Iraq and al-Sham (ISIS), terrorist or military-like activities, or violent acts;

j. Any information that could be determined to passwords, personal identification numbers (PINs), or other information necessary to encrypt or decrypt information;

k. Evidence of geographical location of the cellular telephones at times relevant to the investigation; Global Positioning System (GPS) information and mapping history from any cellular telephones;

l. Evidence of secure storage facilities for financial instruments, passports, visas, and identification documents, including safe deposit boxes;

m. Persons associated with ISIS or involved in terrorist or military-like activities or violent acts overseas or in the United States, including their identities and location and contact information;

n. Contact or communications with organizations whose purpose, primary or ancillary, is raising, collecting, organizing, distributing, or facilitating funds, goods, personnel, or services for training and fighting overseas or in the United States and *not* in conjunction with the U.S. armed forces;

o. Instructions, in any form, relating to explosives, biological weapons, terrorist attacks, or the hacking and other unauthorized use of computers and email and social media accounts; and

p. Hacking or the unauthorized use of any computer or email or social media account.

2. Evidence of user attribution showing who used or owned the cellular telephones at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.